2:24mj9 JCB

AFFIDAVIT

I, Bryant J. Lo Re being duly sworn, hereby depose and state that the following is true to the best of my information, knowledge, and belief:

INTRODUCTION AND AGENT BACKROUND

1. I have been employed as a Police Officer with the West Valley City Police Department since June 6th, 2017, and is currently assigned to the FBI Salt Lake City Field Office's Child Exploitation Task Force as a full-time Task Force Officer. I have been involved in investigations related to the sexual exploitation of children over the internet since July 2020. Since starting my career in Law Enforcement, I have investigated violations of state and federal law, and am currently investigating federal violations concerning child pornography, sexual exploitation of children, and the enticement of children over the internet. I have gained experience through training in seminars, classes, and everyday work related to conducting these types of investigations. I have been involved in numerous investigations involving sex crimes against children, to include leading investigations related to the sexual exploitation of children over the internet, writing and executing search warrants, conducting undercover operations via the internet, interviewing victims, interviewing suspects and conducting arrests.

2. Prior to working as a Task Force Officer with the FBI, I worked as a detective and was assigned to the West Valley City Police Department's Special Victims Unit for four years. I was charged with investigating incidents of adult and juvenile sexual abuse, child abuse and elder abuse in addition to sexual exploitation of children, enticement of children over the internet, and sexual extortion. In 2017, I received a Bachelor's of Science degree in Chemistry and Biology from Westminster University in Salt Lake City, UT.

3. As a federal Task Force Officer, I am authorized to investigate violations of laws of the United States and am a law enforcement officer with the authority to execute warrants issued under the authority of the United States.

PURPOSE OF THE AFFIDAVIT

4. This affidavit is submitted in support of an application for a search warrant for the items described in Attachment A (the "SUBJECT DEVICES,") for the evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Sections 2252/2252A (Possession/Receipt/Access with Intent to View Child Pornography) and 2251 (Production/Attempted Production of Child Pornography) (the "SUBJECT OFFENSES"), more specifically described in Attachment B.

5. Because this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts necessary to support the requested search warrant.

6. The information contained within the affidavit is based on my training and experience, as well as information imparted to me by other law enforcement officers involved in this investigation.

SUMMARY

7. As set forth in detail below, RAUL RAMOS-TERRAZAS has been accused of sexually abusing his 16-year-old niece A.J, who lived with his at his residence in West Valley City, UT. During a forensic interview with A.J. and in addition to multiple instances of sexual abuse, she disclosed that she has found multiple hidden cameras in her bathroom, including one in the shower disguised as a loofa. A residential search warrant was obtained for RAMOS' residence and executed on November 21st, 2023. Approximately 60 pieces of digital media were seized from the house, further described in Attachment A, which included hidden and disguised cameras. In a post-*Miranda* interview, RAMOS admitted to downloading footage off a camera in A.J.'s room and seeing a video of her masturbating. RAMOS admitted the video was still on his primary cell phone and that he has been in possession of this video for 2-3 weeks.

RELEVANT STATUTES

8. This investigation concerns alleged violations of 18 U.S.C. §§ 2252, and 2252A relating to material involving the sexual exploitation of minors.

a) 18 U.S.C. § 2252(a)(4) prohibits possessing one or more books, magazines, periodicals, films, or

other materials which contain visual depictions of minors engaged in sexually explicit conduct that have been transported in interstate or foreign commerce, or that were produced using materials that had traveled in interstate or foreign commerce.

b) 18 U.S.C. § 2252A(a)(1) prohibits knowingly mailing, transporting, or shipping child pornography in interstate or foreign commerce by any means, including by computer.

c) 18 U.S.C. § 2252A(a)(2) prohibits knowingly receiving or distributing any child pornography that has been mailed or shipped or transported in interstate or foreign commerce by any means, including by computer.

d) 18 U.S.C. § 2252A(a)(3)(A) prohibits a person from knowingly reproducing child pornography for distribution through the mail or in interstate or foreign commerce by any means, including by computer.

e) 18 U.S.C. § 2252A(a)(3)(B) prohibits knowingly advertising, promoting, presenting, distributing, or soliciting through the mail, or using any means or facility of interstate or foreign commerce, or in or affecting interstate or foreign commerce by any means any material in a manner that reflects the belief or is intended to cause another to believe that the material is or contains a visual depiction of an actual minor engaging in sexually explicit conduct, or an obscene visual depiction of a minor engaging in sexually explicit conduct.

f) 18 U.S.C. § 2252A(a)(5)(B) prohibits a person from knowingly possessing any book, magazine, periodical, film, videotape, computer disk, or other material that contains an image of child pornography that has been mailed, shipped, or transported in interstate or foreign commerce by any means, including by computer, or that was produced using materials that have been mailed, shipped, or transported in interstate or foreign commerce by any means, including by computer.

DEFINITIONS

9. The following definitions apply to this Affidavit and Attachment B to this Affidavit:

10. "Child Pornography" includes the definition in 18 U.S.C. § 2256(8) (any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct).

11. "Visual depictions" includes prints, copies of visual images, developed and undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image See 18 U.S.C. § 2256(5).

12. "Child Erotica" means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not, in and of themselves, obscene or that do not necessarily depict minors in sexually explicit poses or positions.

13. "IP Address" means Internet Protocol address, which is a unique numeric address used by computers on the Internet. Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

14. "Internet" means a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

15. In this affidavit, the terms "computers" or "digital storage media" or "digital storage devices" may be used interchangeably, and are intended to include any physical object upon which computer data can be

recorded as well as all types of electronic, magnetic, optical, electrochemical, or other high-speed data processing devices capable of performing logical, arithmetic, or storage functions, including desktop and laptop computers, mobile phones, tablets, server computers, game consoles, network hardware, hard disk drives, RAM, floppy disks, flash memory, CDs, DVDs, and other magnetic or optical storage media.

INTRODUCTION REGARDING PREFERENTIAL SEXUAL OFFENDERS AND THE INTERNET

16. Based upon my experience and discussions with other law enforcement officers, your affiant has learned that there are many types of preferential sex offenders. Some of these offenders have a primary sexual interest in children and are often referred to as pedophiles. This affidavit deals with these types of offenders. Preferential sex offenders receive sexual gratification from actual contact with children and/or from fantasy involving children, through the use of photographs and/or digital images that can be stored on computer hard drives and other types of digital recordable media (floppy diskettes, writable compact discs, writable DVDs, etc.). Your affiant is aware that these types of sex offenders often collect sexually explicit material consisting of photographs, video tapes, books, slides, and digital images, which they use for their own sexual gratification and fantasy and to show children in an attempt to lower the child's inhibitions.

17. Your affiant has learned that the Internet has provided preferential sex offenders with a virtually anonymous venue in which they can meet other people with the same or similar sexual interests. Preferential sex offenders also use the computer to electronically exchange pictures of children or of adults engaged in sexual activity with children. These images are readily and easily available on the Internet. These images can then be downloaded and stored on the computer or other forms of digital recordable media such as CD's, DVDs, USB thumb drives, floppy disks, etc., and then viewed on the computer monitor at any time. Preferential sex offenders will also participate in chat rooms in order to communicate with other like-minded individuals and to meet children. This communication serves to legitimize their conduct and beliefs. Your affiant also knows from training and experience that preferential sex offenders who collect child pornography

rarely, if ever, dispose of their sexually explicit materials and may go to great lengths to conceal and protect from discovery, theft, and damage to their collections of child pornography. I also know that these individuals typically maintain their child pornography collections in the privacy and security of their homes, or other secure location.

BACKGROUND REGARDING THE INTERNET AND CHILD EXPLOITATION

18. I have been formally trained in the investigation of crimes involving the sexual exploitation of children. I also own my own computer, have personal knowledge of the operation of a computer, and have accessed the Internet for numerous years. Based on this training and knowledge, and the experience of other law enforcement personnel involved in this investigation, I know the following:

19. Child pornographers can produce images using a wireless device such as a cell phone. Photos can also be made using cameras, then can be transferred onto another device either using wire or wireless technology. Images can also be uploaded to Internet-based storage commonly referred to as the "cloud." Hard-copy images can also be scanned into a computer. Via the Internet, connection can be made to literally millions of computers around the world. Child pornography can be transferred quickly and easily via electronic mail or virtually countless other online platforms, communication services, storage services, and applications.

20. A computer's capability to store images in digital form makes it an ideal repository for child pornography and other files related to the sexual abuse and exploitation of children. The digital-storage capacity in devices and in the "cloud" has grown tremendously within the last several years. Thumb drives with a capacity of 32 gigabytes are not uncommon. Flash cards with a capacity of 32 gigabytes are not uncommon. Hard drives with the capacity of 500 gigabytes up to 3 terabytes are not uncommon. Phones with over 100 gigabytes in storage are not uncommon. Devices can store thousands of images and videos at very high resolution. These devices are often internet capable and can not only store, but can transmit images via the internet and can use the devices to store images and documents in internet or "cloud" storage spaces. Once this is done, there is no readily apparent evidence at the "scene of the crime". Only with careful laboratory

examination of electronic storage devices is it possible to recreate the evidence trail.

21. With Internet access, a computer user can transport an image file from the Internet or from another user's computer to his own computer, so that the image file is stored in his computer. The process of transporting an image file to one's own computer is called "downloading". The user can then display the image file on his computer screen, and can choose to "save" the image on his computer and/or print out a hard copy of the image by using a printer device (such as a laser or inkjet printer). Sometimes the only method to recreate the evidence trail of this behavior is with careful laboratory examination of the computer, modem, printer, and other electronic devices.

22. I know from training and experience that search warrants of residences involved in computer or digitally related criminal activity usually produce items that tend to establish ownership or use of digital devices and ownership or use of any Internet service accounts accessed to obtain child pornography to include credit card bills, telephone bills, correspondence and other identification documents.

23. I know from training and experience that search warrants of residences usually reveal items that tend to show dominion and control of the property searched, to include utility bills, telephone bills, correspondence, rental agreements and other identification documents.

INDIVIDUALS WHO HAVE A SEXUAL INTEREST IN CHILDREN AND RECEIVE AND/OR DISTRIBUTE CHILD PORNOGRAPHY

24. Based on the facts set forth below, there is probable cause to believe that RAMOS-TERRAZAS is someone with a sexual interest in children and images of children. Based on my previous training and experience related to investigations involving child pornography and the sexual abuse of children, I have learned that individuals like RAMOS-TERRAZAS who have a sexual interest in children/images of children, there are certain characteristics commonly found in these individuals:

a. The majority of individuals who create and collect child pornography are persons who have a sexual

attraction to children. They receive sexual gratification and satisfaction from sexual fantasies fueled by depictions of children that are sexual in nature

b. Individuals who create and collect child pornography collect sexually explicit materials, which may consist of photographs, magazines, motion pictures, video tapes, books, slides, computer graphics or digital or other images for their own sexual gratification.

c. These individuals often also collect child erotica, which may consist of images or text that do not rise to the level of child pornography but which nonetheless fuel their deviant sexual fantasies involving children. Non-pornographic, seemingly innocuous images of minors are often found on computers and digital storage devices that also contain child pornography, or that is used to communicate with others about sexual activity or interest in children. Such images are useful in attempting to identify actual minors depicted in child pornography images found during the execution of a search warrant. In certain cases, such images may also assist in determining the origins of a particular child pornography image or series of images.

d. Many individuals who create and collect child pornography rarely, if ever, dispose of their sexually explicit materials and may go to great lengths to conceal and protect from discovery, theft, and damage their collections of illicit materials. They regularly maintain their collections in the privacy and security of their homes, cars, garages, sheds, or other secure storage location, such as on their person. Many also frequently delete their collection of child pornography, as well as wipe their digital devices in an attempt to destroy evidence and evade law enforcement.

e. Individuals who create and collect child pornography often seek out like-minded individuals, either in person or on the Internet, to share information and trade depictions of child pornography and child erotica as a means of gaining status, trust, acceptance and support. This contact helps these individuals to rationalize and validate their deviant sexual interest and associated behavior. The different Internet-based vehicles used by such individuals to communicate with each other include,

but are not limited to, e-mail, e-mail groups, bulletin boards, IRC, newsgroups, instant messaging, and other similar vehicles.

f. Individuals who create and collect child pornography often maintain books, magazines, newspapers and other writings, in hard copy or digital medium, on the subject of sexual activities with children, as a way of understanding their own feelings toward children, justifying those feelings and finding comfort for their illicit behavior and desires. Such individuals rarely destroy these materials because of the psychological support they provide.

g. Individuals who create and collect child pornography often collect, read, copy or maintain names, screen names or nicknames, addresses (including e-mail addresses), phone numbers, or lists of persons who have advertised or otherwise made known in publications and on the Internet that they have similar sexual interests. These contacts are maintained as a means of personal referral, exchange or commercial profit. These names may be maintained in the original medium from which they were derived, in telephone books or notebooks, on computer storage devices, or merely on scraps of paper.

25. Based upon training and experience, I know that persons in engaged in the production and possession of child erotica are also often involved in the production and possession of child pornography. Likewise, I know from training and experience that persons involved in the production and possession of child pornography are often involved in the production and possession of child erotica.

26. Based on my training, knowledge, experience, and conversations with others in law enforcement, I understand that an individual who possesses images and/or videos depicting child pornography on one digital storage devices and/or Internet email or online storage account is likely to possess child pornography on additional digital storage devices and/or Internet email or online storage accounts that s/he possesses. Additionally, based on this training and experience, I understand that an individual who discusses the sexual abuse and/or exploitation of children on one digital storage device is likely to conduct those communications on

additional digital storage devices that s/he possesses.

SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS

30. Searches and seizures of evidence from computers commonly require agents to download or copy information from the computers and their components or seize most or all computer items (computer hardware, computer software, and computer related documentation) to be processed later by a qualified computer expert in a laboratory or other controlled environment. This is almost always true because of the following:

a. Computer storage devices (like hard disks, diskettes, tapes, laser disks, magneto opticals, and others) can store the equivalent of thousands of pages of information. Especially when the user wants to conceal criminal evidence, he or she often stores it in random order with deceptive file names. This requires searching authorities to examine all the stored data to determine whether it is included in the warrant. This sorting process can take days or weeks, depending on the volume of data stored, and it would be generally impossible to accomplish this kind of data search on site; and

b. Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert should analyze the system and its data. The search of a computer system is an exacting scientific procedure which is designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to tampering or destruction (which may be caused by malicious code or normal activities of an operating system), the controlled environment of a laboratory is essential to its complete and accurate analysis.

31. In order to fully retrieve data from a computer system, the analyst needs all magnetic storage

additional digital storage devices that s/he possesses.

SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS

30. Searches and seizures of evidence from computers commonly require agents to download or copy information from the computers and their components or seize most or all computer items (computer hardware, computer software, and computer related documentation) to be processed later by a qualified computer expert in a laboratory or other controlled environment. This is almost always true because of the following:

a. Computer storage devices (like hard disks, diskettes, tapes, laser disks, magneto opticals, and others) can store the equivalent of thousands of pages of information. Especially when the user wants to conceal criminal evidence, he or she often stores it in random order with deceptive file names. This requires searching authorities to examine all the stored data to determine whether it is included in the warrant. This sorting process can take days or weeks, depending on the volume of data stored, and it would be generally impossible to accomplish this kind of data search on site; and

b. Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert should analyze the system and its data. The search of a computer system is an exacting scientific procedure which is designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to tampering or destruction (which may be caused by malicious code or normal activities of an operating system), the controlled environment of a laboratory is essential to its complete and accurate analysis.

31. In order to fully retrieve data from a computer system, the analyst needs all magnetic storage

devices as well as the central processing unit (CPU). In cases involving child pornography where the evidence consists partly of graphics files, the monitor(s) may be essential for a thorough and efficient search due to software and hardware configuration issues. In addition, the analyst needs all the system software (operating systems or interfaces, and hardware drivers) and any applications software which may have been used to create the data (whether stored on hard drives or on external media).

32. In addition, there is probable cause to believe that the computer and its storage devices, the monitor, keyboard, and modem are all instrumentalities of the crime(s), within the meaning of 18 U.S.C. §§ 2251, 2252, 2252A, 2422, and 2423 and should all be seized as such.

SEARCH METHODOLOGY TO BE EMPLOYED

33. The search procedure of electronic data contained in computer hardware, computer software, and/or memory storage devices may include the following techniques (the following is a non-exclusive list, as other search procedures may be used):

a. examination of all of the data contained in such computer hardware, computer software, and/or memory storage devices to view the data and determine whether that data falls within the items to be seized as set forth herein;

b. searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth herein (any data that is encrypted and unreadable will not be returned unless law enforcement personnel have determined that the data is not (1) an instrumentality of the offenses, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) evidence of the offenses specified above);

c. surveying various file directories and the individual files they contain;

d. opening files in order to determine their contents;

e. scanning storage areas;

f. performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are likely to appear in the evidence described in Attachment A; and/or

g. performing any other data analysis technique that may be necessary to locate and retrieve the evidence described in Attachment B.

PROBABLE CAUSE

31. The following is based on my knowledge and experience, and on information received from other individuals, including law enforcement officers, as well as their reports:

32. On October 27th, 2023 the West Valley City Police Department received a report from a citizen witness, whose identity is known to law enforcement and whose identity can be disclosed to the Court upon request, about her female minor relative (hereinafter referred to as Victim 1) being sexually abused by a relative of the citizen witness, RAUL RAMOS-TERRAZAS. Victim 1 explained to Officer Campas that RAMOS-TERRAZAS had taken her for a driving lesson in West Valley City, UT when he stuck his hand down her pants and touched her vagina.

33. A Child Forensic Interview was completed with Victim 1 on November 6th, 2023 at the South Valley Children's Justice Center in Salt Lake County, Utah. Victim 1 disclosed the following information during her interview:

i. Victim 1 is related to RAMOS-TERRAZAS.

ii. Victim 1 previously lived in the same home as RAMOS-TERRAZAS.

iii. Beginning when Victim 1 was in the 7th grade, RAMOS-TERRAZAS would come into her room at night and touch her vagina over her clothes while Victim 1 was asleep. This would happen almost every night. Victim 1 recalled two specific times that it was light enough in

her room that she could see RAMOS-TERRAZAS leaving her room after touching her vagina.

iv. RAMOS-TERRAZAS recently started teaching Victim 1 how to drive and would take her out into empty parking lots for driving lessons. During these lessons, Victim 1 would have to sit on RAMOS-TERRAZAS's lap in the driver seat.

v. On October 27th, 2023 RAMOS-TERRAZAS took Victim 1 out for a driving lesson in West Valley City. Victim 1 was sitting on RAMOS-TERRAZAS's lap like usual. RAMOS-TERRAZAS began rubbing Victim 1's legs, unbuttoned her pants, put his hand inside her pants and underwear and digitally penetrated her vagina. Victim 1 said RAMOS-TERRAZAS apologized to her when they got back home.

vi. Victim 1 also disclosed that, in the past year, she has found multiple hidden cameras in her bathroom, including a camera in the shower disguised as a loofa. She has also found disguised cameras on the bathroom counter and hidden under the sink.

34. The citizen witness was interviewed by Det. Lougy on November 6th, 2023 and provided the following information:

i. The citizen witness has been Victim 1's guardian since Victim 1 was about 8 years old. Victim 1 started living with the citizen and RAMOS-TERRAZAS at their residence in West Valley City, UT when Victim 1 was around 11 years old.

ii. The citizen witness was in California when Victim 1 disclosed the abuse to the citizen witness. The citizen witness flew back to Utah and spoke with Victim 1, who said that RAMOS-TERRAZAS had touched her vagina while they were doing a driving lesson. RAMOS-TERRAZAS ended his relationship with the citizen witness.

iii. The citizen recalled that approximately one year ago, her now 14-year-old daughter and Victim 1 told her that they found a hidden camera in the bathroom. The citizen confronted

RAMOS-TERRAZAS about the hidden camera. RAMOS-TERRAZAS said that someone from a recent party must have put the camera in the bathroom.

35. On November 21st, 2023 a search warrant for RAMOS-TERRAZAS's residence was obtained and executed by several members of the West Valley City Police Department. RAMOS-TERRAZAS was arrested without incident. A total of 60 items of evidence were seized from the residence, including multiple cell phones, computers, hidden and disguised cameras, SD cards, hard drives and other digital storage media.

36. In a post *Miranda* interview, RAMOS-TERRAZAS provided the following information:

i. RAMOS-TERRAZAS recently broke up with the citizen witness because he thought she was cheating on him. They had been together for 12-13 years. Victim 1 has been living with RAMOS-TERRAZAS for the last five years.

ii. RAMOS-TERRAZAS admitted to taking Victim 1 for driving lessons but denied sexually abusing her. RAMOS-TERRAZAS said the first time he took her driving, he had her sit on his lap so he could control the brake and accelerator.

iii. RAMOS-TERRAZAS admitted to finding a camera hidden in Victim 1's bedroom approximately 2-3 weeks ago. RAMOS-TERRAZAS looked the device up and found an app that can be used to download footage off the camera. RAMOS-TERRAZAS found a video of Victim 1 masturbating and saved it to his phone, claiming he was going to show the child's guardian. RAMOS-TERRAZAS said the video was still on his primary cell phone, a Samsung Note 20+.

37. At the time the search of RAMOS-TERRAZAS's home was conducted, a large number of devices, more particularly described in Attachment B, were found within the home. Some of these devices are cameras which may have been used in the surreptitious recording of the child. Other devices are devices with memory chips or hard drives which could be used to access these cameras or store data obtained from these cameras.

38. I know based on training and experience that it is not uncommon for people who create or possess child pornography to hide that contraband on a variety of storage mediums, include cell phones or computers no longer in continual use by others, in an attempt to prevent the inadvertent discovery of that contraband by other people.

CONCLUSION

39. Based on the investigation described above, probable cause exists to believe that evidence, fruits and instrumentalities of the SUBJECT OFFENSES will be located on the SUBJECT DEVICES. I, therefore, respectfully request that the attached warrant be issued authorizing the search and seizure of the items listed in Attachment B.

I declare under penalty of perjury that the foregoing is true and correct to the best of my information, knowledge, and belief.

Bryant LoRe Digitally signed by Bryant LoRe Date: 2024.01.04 11:24:33 -07'00'

Bryant J. Lo Re
Detective, West Valley Police Department
Task Force Officer, Federal Bureau of Investigation

SUBSCRIBED and SWORN before me this 4th day of January, 2024.

UNITED STATES MAGISTRATE JUDGE